REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is directed to non-statutory subject matter under 35 U.S.C. §101, anticipated under the provisions of 35 U.S.C. §102, or obvious under the provisions of 35 U.S.C. §103. Thus, the Applicants believe that all of these claims are in allowable form.

I. REJECTION OF CLAIMS 10, 12, AND 13 UNDER 35 U.S.C. §101

Claims 10, 12, and 13 stand rejected as being allegedly directed to non-statutory subject matter. Specifically, the Examiner alleges that "the applicant has not shown that the computer readable medium [recited in claims 10, 12, and 13] is hardware" (Final Office Action, Page 2). The Applicants respectfully traverse the rejection. Moreover, the Applicants note that claim 13 was cancelled without prejudice in a previous amendment; accordingly, the rejection of claim 13 is moot.

Specifically, the Applicants respectfully submit that the claims 10 and 12 were amended in a previous response to recite a "computer readable storage medium" (emphasis added). "In this context, 'functional descriptive material' consists of data structures and computer programs which impart functionality when employed as a computer component." (MPEP 2106.01) "When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized." (MPEP 2106.01)

Since the claimed executable program is contained on a computer readable storage medium, the executable program is "structurally and functionally interrelated" to the computer readable storage medium, and, as such, is statutory in accordance with MPEP 2106.01.

Moreover, the Board of Patent Appeals and Interferences recently noted in *Ex parte Bo Li*, 2008-1213, that "Beauregard" claims are viewed as product claims, and are therefore statutory under 35 U.S.C. §101. *See Bo Li* at Page 9 ("It has been the practice for a number of years that a 'Beauregard Claim' ... be considered statutory at the USPTO as a product claim. (MPEP 2105.01, I). Though not finally adjudicated, this practice is not inconsistent with *In re Nuijten*. (*Ibid*)"). The Board further noted that a

combination of software components embodied upon a computer readable medium "has been found statutory under the teachings of *In re Lowry*, 32 F.3d 1579 (Fed. Cir. 1994)." (*Bo Li* at Page 9). The Applicants respectfully submit that the holding of the Board in *Ex parte Bo Li* therefore supports a finding that the subject matter embodied in claims 10 and 12 is statutory.

Therefore, the Applicants respectfully submit that claims 10 and 12 fully satisfy the requirements of 35 U.S.C. §101. Accordingly, the Applicants respectfully request that the rejection under 35 U.S.C. §101 be withdrawn.

II. REJECTION OF CLAIMS 1-2, 4-5, AND 10-13 UNDER 35 U.S.C. § 102

Claims 1-2, 4-5, and 10-13 stand rejected as being anticipated by the Purtell et al. patent (U.S. 6,950,947, issued September 27, 2005, hereinafter "Purtell"). Claim 13 has been cancelled without prejudice, as discussed above. Applicants respectfully traverse the remaining rejections.

Particularly, the Examiner's attention is directed to the fact that Purtell fails to disclose or suggest a method for correlating sensors in an intrusion detection system by adjusting a belief state of a first sensor based on a belief state of a second sensor, where the belief states indicate probabilistic beliefs of the sensors regarding states of system resources or services, as claimed in Applicants' independent claims 1, 4, 5, and 10 - 12.

By contrast, Purtell discloses a set of peer firewalls that share direct measurements of transmission control protocol (TCP) control state. Specifically, the firewalls exchange common TCP control blocks (CCBs) that contain objective information about the physical connection between two entities connected via TCP (such as "round trip time (RTT) and variance, the congestion-controlled window, local and remote MSS [maximum segment size], and retransmission and error rate," Purtell, column 4, lines 15-19). Thus, the shared data is not probabilistic, as claimed by the Applicants, but rather has definite, directly measured values.

Specifically, Applicants' claims 1, 4, 5, and 10 - 12 positively recite:

1. A method for correlating a first sensor to a second sensor in an intrusion detection system, the first sensor and the second sensor each maintaining belief

regarding a resource or service monitored by the intrusion detection system, the method comprising the steps of:

(a) transmitting to the first sensor information about a belief state of the second sensor, said belief state of the second sensor indicating a probabilistic belief regarding a state of at least one system resource or service directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a probabilistic belief regarding a state of at least one system resource or service directly monitored by the first sensor, the adjusting based at least in part on the belief state of the second sensor, so that a sensitivity of the first sensor to suspicious activity in the intrusion detection system is improved. (Emphasis added)

4. A method for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a state of a resource monitored by the intrusion detection system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of a probabilistic belief of the second sensor regarding an apparent normal, degraded or compromised state of a resource directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a probabilistic belief regarding an apparent normal, degraded or compromised state of a resource directly monitored by the first sensor, so that an erroneous transaction with the degraded or compromised resource does not generate an alarm in the intrusion detection system. (Emphasis added)

5. A method for enhancing a sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a service monitored by the intrusion detection system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of a belief state of the second sensor indicating a probabilistic belief regarding an existence or validity of services supported on computer system resources directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a probabilistic belief regarding an existence or validity of services supported on computer system resources directly monitored by the first sensor so that an attempted communication with a nonexistent system service or resource appears suspicious to the intrusion detection system. (Emphasis added)

10. A computer readable storage medium containing an executable program for correlating a first sensor to a second sensor in an intrusion detection system, the first sensor and the second sensor each maintaining belief regarding a resource or service monitored by the intrusion detection system, where the program performs the steps of:

(a) transmitting to the first sensor information about a belief state of the

second sensor, said belief state of the second sensor indicating a probabilistic belief regarding a state of at least one system resource or service directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a probabilistic belief regarding a state of at least one system resource or service directly monitored by the first sensor, the adjusting based at least in part on the belief state of the second sensor, so that a sensitivity of the first sensor to suspicious activity in the intrusion detection system is improved. (Emphasis added)

11. A computer readable storage medium containing an executable program for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a state of a resource monitored by the intrusion detection system, where the program performs the steps of:

(a) transmitting to the first sensor all or part of a probabilistic belief of the second sensor regarding an apparent normal, degraded or compromised state of a resource directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a probabilistic belief regarding an apparent normal, degraded or compromised state of a resource directly monitored by the first sensor so that an erroneous transaction with the degraded or compromised resource does not generate an alarm in the intrusion detection system. (Emphasis added)

12. A computer readable storage medium containing an executable program for enhancing a sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a service monitored by the intrusion detection system, where the program performs the steps of:

(a) transmitting to the first sensor all or part of a belief state of the second sensor indicating a probabilistic belief regarding an existence or validity of services supported on computer system resources directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a probabilistic belief regarding an existence or validity of services supported on computer system resources directly monitored by the first sensor so that an attempted communication with a nonexistent system service or resource appears suspicious to the intrusion detection system. (Emphasis added)

As discussed above, Purtell fails to disclose or suggest a method for correlating sensors in an intrusion detection system by adjusting a belief state of a first sensor based on a belief state of a second sensor, where the belief states indicate probabilistic beliefs of the sensors regarding states of system resources or services, as claimed in Applicants' independent claims 1, 4, 5, and 10 - 12. Therefore, the Applicants submit

that independent claims 1, 4, 5, and 10 - 12 fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

Dependent claim 2 depends from claim 1 and recites additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claim 2 is not anticipated by the teachings of Purtell. Moreover, Purtell fails to teach or suggest the method of claim 1, wherein the first and second sensors are different types of sensors, as recited by Applicants' claim 2. By contrast, Purtell teaches a system in which devices of the same type (*i.e.*, firewalls) share data (TCP control blocks). There is no suggestion anywhere in Purtell that the shared data is provided to any devices other than the firewalls. The portion of Purtell that the Examiner cites to teach the feature of first and second sensors that are different types of sensors at best teaches that the firewalls may be proxy servers, which are merely a specific type of firewall (*See, e.g.*, Purtell, column 1, lines 41-43: "A common type of firewall is a proxy server...," emphasis added). Moreover, Purtell suggests that in a preferred embodiment, all of the firewalls are proxy servers ("In a preferred embodiment, the firewalls are configured as proxy servers," Purtell, column 3, lines 33-34). Nowhere in Purtell is it suggested that the firewalls comprise a mix of firewalls and other devices, or a mix of proxy servers and other devices. Therefore, the Applicants submit that dependent claim 2 also fully satisfies the requirements of 35 U.S.C. §102 and is patentable thereunder.

III. REJECTION OF CLAIM 3 UNDER 35 U.S.C. § 103

Claim 3 stands rejected as being unpatentable over Purtell in view of the Timm patent (U.S. 5,440,498, hereinafter "Timm"). The Applicants respectfully traverse the rejection.

As discussed above, Purtell does not teach or even suggest a method for correlating sensors in an intrusion detection system by adjusting a belief state of a first sensor based on a belief state of a second sensor, where the belief states indicate probabilistic beliefs of the sensors regarding states of system resources or services, as claimed in Applicants' independent claim 1, from which claim 3 depends. Applicants' claim 1 has been recited above. Timm does not bridge this gap in the teachings of Purtell. Specifically, Timm teaches that the elements of a security system are evaluated

in order to "quantify[ ] the relative capabilities of the elements to protect the facility" (Timm, column 1, line 68 – column 2, line 2, emphasis added). In other words, the probabilities represent the likelihood that a sensor will detect an event (*i.e.*, an intrusion). This stands in contrast to the claimed invention, where the probabilistic beliefs associated with the sensors represent the likelihood that a state of a system service or resource is of a certain nature (*e.g.*, normal, degraded, compromised, valid, etc.).

Purtell and Timm, singularly or in any permissible combination, thus fail to teach, suggest all of the features of Applicants' independent claim 1. Therefore, the Applicants submit that independent claim 1 fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

Dependent claim 3 depends from claim 1 and recites additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claim 3 is not made obvious by the teachings of Purtell in view of Timm. Therefore, the Applicants submit that dependent claim 3 also fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

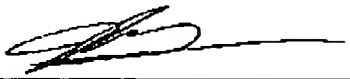
IV. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §101, 35 U.S.C. §102 and 35 U.S.C. §103. Consequently, the Applicants believe that all of these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the maintenance of the final action in any of the claims now pending in the application, it is requested that the Examiner telephone Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

09/711,323

Respectfully submitted,



December 11, 2008
Date

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702